PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/20 — A1

(11) International Publication Number: WO 95/34177

(43) International Publication Date: 14 December 1995 (14.12.95)

(21) International Application Number: PCT/US95/07251

(22) International Filing Date: 7 June 1995 (07.06.95)

(30) Priority Data:
08/225,341 7 June 1994 (07.06.94) US

(71) Applicant *(for all designated States except US)*: CELSAT AMERICA, INC. [US/US]; Suite 220, 3460 Torrance Boulevard, Torrance, CA 90503 (US).

(72) Inventor; and

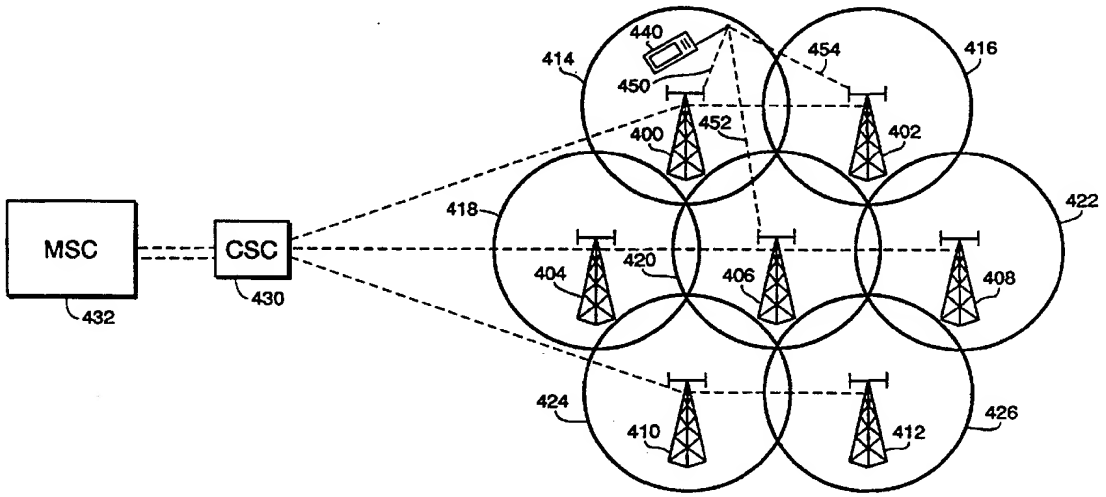
(75) Inventor/Applicant *(for US only)*: OTTEN, David, D. [US/US]; 532 South Gertruda, Redondo Beach, CA 90277 (US).

(74) Agent: DRUMMOND, William, H.; Drummond & Duckworth, Suite 500, 4590 MacArthur Boulevard, Newport Beach, CA 92660 (US).

(81) Designated States: CA, CN, JP, RU, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: FRAUD DETECTION IN A CELLULAR COMMUNICATIONS SYSTEM



(57) Abstract

Apparatus and methods for operating a wireless communications system provided for reducing the use of the system by unauthorized users by establishing the geographical location of a selected user (440), comparing this location with the known locations of authorized users and denying service to the selected user if the selected user's location does not correspond to the known location of authorized users.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

FRAUD DETECTION IN A CELLULAR COMMUNICATIONS SYSTEM

BACKGROUND

This invention relates to improvements in mobile wireless communication systems.

In another respect, the invention relates to communication systems such as a cellular mobile communications system having integrated satellite and ground nodes.

More particularly, the invention pertains to mobile wireless communications systems which can locate and/or disable the communications equipment of a fraudulent user of the system.

The cellular communications industry has grown at a fast pace in the United States and even faster in some other countries. In the cellular communications industry alone, it is estimated that the number of mobile subscribers will increase on a world-wide level by an order of magnitude within the next ten years. In order to meet the world's ever-increasing demand for mobile communications, numerous diverse systems have been devised. For example, mobile communications system such as Specialized Mobile Radio (SMR), the planned Personal Communications Service (PCS) and existing cellular radio

are primarily aimed at providing mobile telephone service to automotive users in developed metropolitan areas. For remote area users, airborne users, and marine users, AIRFONE and INMARSAT services exist but coverage is incomplete and/or service is relatively expensive. Mobile radio satellite systems in an advanced planning stage will probably provide improved direct-broadcast voice channels to mobile subscribers in remote areas but still at significantly higher cost in comparison to existing ground cellular service. The ground cellular and planned satellite technologies complement one another in geographical coverage in that the ground cellular communications service provides voice and data telephone service in relatively developed urban and suburban areas but not in sparsely populated areas, while the planned earth orbiting satellites will serve the sparsely populated areas.

In the case where one band of frequencies is preferable over others and that one band alone is to be used for mobile communications, efficient communications systems are necessary to assure that the number of users desiring to use the band can be accommodated. For example, there is presently widespread agreement on the choice of L-band as the technically preferred frequency band for the satellite-to-mobile link in mobile communications systems.

To meet the world's demand for additional mobile communications capabilities, more communications systems will need to be employed. An additional technology that is anticipated to find widespread application in mobile wireless communications systems is the spread spectrum communications technique. The spread spectrum communications technique is a technology that has found widespread use in military applications which must meet requirements for security, minimized likelihood of signal detection, and minimum susceptibility to external interference or jamming. In a spread spectrum system, the data modulated carrier signal is further modulated by a relatively wide-band, pseudo-random "spreading" signal so that the transmitted bandwidth is much greater than the bandwidth or rate of the information to be transmitted. Commonly the "spreading" signal is generated by a pseudo-random deterministic digital logic algorithm which is duplicated at the receiver.

By further modulating the received signal by the same spreading waveform, the received signal is remapped into the original information bandwidth to reproduce the desired signal. Because a receiver is responsive only to a signal that was spread using the same unique spreading code, a uniquely addressable channel is possible. Also, the power spectral density is low and without the unique spreading code, the signal is very difficult to detect, much less decode, so privacy is enhanced and interference

with the signals of other services is reduced. The spread spectrum signal has strong immunity to multipath fading, interference from other users of the same system, and interference from other systems.

Unfortunately, accompanying the rapid growth of mobile communications technology has been corresponding growth in the fraudulent procurement of mobile communications. Already, signal theft, also known as "pirating," or "cellular fraud," is a major problem in current cellular systems.

Cellular fraud is a serious problem in the cellular industry, not only in the United States but worldwide. In 1994 cellular fraud accounted for $500M of lost revenue in the United States and $1 billion worldwide. Currently, every month an additional 50,000 cellular telephone numbers are stolen and illegally used in the United States. Cellular fraud is thus equivalent to 2.5% of the total annual revenue of the United States cellular industry for 1994 ($20 billion) and it is rising every year. Some cellular carriers in the largest United States cities have been hit extremely hard by fraud, including one large US carrier who lost $40M in one three month period, when 600 cellular phones were illegally activated, without being detected by the operator. Internationally, some cellular operators in less developed countries have experienced fraud as high as 30%

on their networks, because they have not installed adequate credit checking controls or fraud prevention procedures.

The United States Secret Service considers the stealing of cellular telephone numbers as counterfeiting (Title 18, Section 1029) and as such, it is a Federal offense with penalties rising as high as a fine of $100,000 and 20 years imprisonment. Organized criminals including drug dealers and gangs, car thieves and armed robbers use counterfeit cellular phones widely because cellular phones provide the criminal with communications mobility as well as anonymity. Thus the police often find that when they catch organized criminals, counterfeit phones are also recovered. In the last two years, over 500 suspects have been arrested for counterfeiting cellular phones and thousands of stolen phones have been recovered by the United States Secret Service and Federal Bureau of Investigation. Notwithstanding, the number of counterfeit phones is growing rapidly.

Pirating can be accomplished in several manners. In particular, there are three basic classifications of cellular fraud described herein as "Access Fraud", "Subscription Fraud" and "Stolen Phone Fraud." Essentially all types of cellular access fraud involve the perpetrators or "Bandits" making cellular calls on

counterfeit cellular phones, whose electronic identity has been illegally modified to resemble that of another valid or non-existent subscriber's cellular phone.

In order for a subscriber to make a call on his home cellular network, his subscriber unit's cellular phone number/electronic serial number (ESN) combination must correspond exactly with the phone and electronic serial and numbers stored in the cellular operator's cellular telephone exchange. If the numbers do not correspond, then the cellular system will not complete the subscribers call.

Access fraud is the unauthorized use of cellular service through changing of a cellular phone's unique Electronic Serial Number (ESN) and/or the subscriber's phone number or Mobile Identification Number (MIN). Presently, pirates manage to acquire the authorization code intended to restrict system use to the authorized customers for whom it was intended. A mobile user unit is then altered to incorporate the stolen authorization code enabling the altered pirate user unit to transmit and receive signals of the communications system in the same manner as the lawful subscriber of the cellular system to whom had been originally appointed the authorization code. In this manner, it is extremely common for a fraudulent user to unlawfully use the

communications system charging all communications to an innocent subscriber.

Further, access fraud has several variants including the most common, tumbling ESN/MIN & Counterfeiting (Cloning). Tumbling ESN/MIN involves the modification of a mobile unit's unique ESN/MIN combination. The phone is modified such that the ESN/MIN identity for a pseudo "roamer" is changed whether randomly or sequentially after every call to that of another roaming subscriber's unit. A roamer is a cellular subscriber who uses his cellular phone in another market, i.e., a New York "Nynex Mobile" subscriber who visits Chicago and makes and receives calls on his phone using the local "Ameritech Mobile" network.

The constant alteration of the counterfeit phone's ESN and/or MIN allows the bandit to evade the detection and "shut down" of that phone. This is because, in the less sophisticated cellular systems, there is no way of telling whether the roamer caller is a valid roamer subscriber or not and so tumbling fraud cannot be immediately detected. This authentication is known as "Pre-Call Subscriber ESN/MIN validation".

Cloning, or counterfeiting, occurs when the bandit obtains valid subscriber's ESN/MIN combinations, usually by monitoring ("scanning") cellular radio transmission

"over the air" using special cellular radio signaling data receivers and decoders. The bandit then programs these ESN/MIN's into his phone, thus appearing to the cellular operator as a valid subscriber. the bandit continues to place illegal calls on his cellular phones until detected. This detection often occurs only after the valid subscriber calls up the cellular operator's Customer Car department to complain that his monthly bill contains calls which he did not make. At this time the counterfeited ESN/MIN combination is denied service. Additionally, the valid subscriber is also denied service and must have his MIN (cellular telephone number) changed in order to have his service restored causing additional inconvenience.

"Subscription fraud" occurs when a subscriber signs up for service with fraudulent identification, without any intention of paying for the service. An example of subscription fraud occurs when a bandit subscriber fraudulently uses the credit card number, social security number, state drivers license, or other means of identification, of another in an effort to obtain the use of a cellular communications system. The bandit then uses the system without paying until the bills have mounted to the point that their authorization is discontinued by the cellular provider. This cycle is then repeated using the identification of another innocent individual. Unfortunately, this type of

cellular fraud is particularly widespread and costly, incurring millions of dollars of losses to both the cellular industry and those innocent individuals whose means of identification has been purloined.

Simply, "stolen phone" fraud occurs when a legitimate phone is stolen and used before it can be denied service. The pirate merely steals a user unit already including the authorization code of a subscriber. Unfortunately, by the very nature of the cellular units being lightweight, readily concealable and mobile has created a low risk, high profit market for theft. Further, a subscriber, often believing that they have merely misplaced their user unit, will often wait weeks or even months before realizing that their user unit has been stolen. Accordingly, the subscriber often does not notify their mobile communications provider to cease cellular services until thousands of dollars worth of cellular communications have been pirated. The pirate does not pay the fees due to the service provider and the costs are transferred either to the subscriber of the stolen authorization code or to the users of the system as a whole.

Unfortunately, due to the threat of cellular fraud, many cellular operators now limit the ability of cellular subscribers to use their cellular phones to make long distance and international calls, particularly

residential and roaming subscribers. This limits the revenue opportunities for the cellular operator. If cellular fraud could be more easily detected and combated, then cellular operators could lift these calling restrictions, increasing the utility of the phones to the subscribers and raising the average monthly revenue for the operators.

In an effort to eliminate cellular fraud, numerous fraud detection techniques have been attempted. The first of these, "call pattern analysis" entails the review of a subscribers cellular velocity, volume, duration, destination, and initial bill credit limit. Special software in a billing server analyzes a very large number of call detail records (e.g., 3 month's worth) from the cellular telephone exchange to look for anomalies and changes in patterns of: 1) call origination location with respect to time, e.g., to look for phones with the same MIN/ESN being used at the same time in two different places (also known as "Velocity"); 2) call volume, e.g., the subscriber starts to use very high volumes of airtime minutes when their previous volume was low; 3) call duration, which may indicate that the phone is being used as a "free long distance pipeline" for calls forwarded to that MIN; 4) call destination, e.g., if a subscriber starts making large numbers of international calls when the previous international activity was low; 5) call time, e.g., the subscriber

starts using high volumes of nighttime minutes whereas previously all the usage was during the day. The same software is also programmed to detect very high calling volumes in the initial few days and weeks after the services is activated when no pattern data is available. This often detects when a subscriber has no intention of paying the bill.

An additional fraudulent detection means has been called "Dual Call Set-Up Logs." Special software in the cellular telephone exchange identifies any situation with an alarm log when two subscriber units with identical MIN/ESN combinations attempt to have simultaneous phone calls on the same cellular switch.

Some cellular systems include the fraudulent detection means "Dual Phone Page Responses." When a cellular phone number is dialled and two units respond to the "page" on different cellsites and different frequencies at the same time. The switch identifies that two separate and distinct mobiles with the same MIN/ESN combination have the responded to a page and issues an alarm log that a fraudulent user is using the system.

"Tumbling ESN Analysis" is a fraud detection system where the cellular telephone exchange looks for patterns in MIN/ESN combinations as well as patterns in MIN/ESN combination tumbling and issues an alarm log if tumbling is detected.

A somewhat ingenious system for detecting cellular fraud, though hardware intensive and somewhat expensive, is "Subscriber Unit Fingerprinting." Special receivers at each base station, characterize the FM transmission of each cellular telephone, e.g., the exact FM deviation, carrier frequency, data modulation frequency, etc. on the call set-up channels of the network. If cellular telephones with identical ESN/MIN combinations and different radio characteristics are identified, a cloned unit is detected.

In addition to detecting a cellular fraud realtime, increased analysis of presently provided information has been employed to reduce cellular fraud. For example, subscribers are asked to examine their monthly bill and document those calls that appear on their bills which they did not make. Subscribers are then asked to call the cellular operators' billing department to get the fraudulent calls removed, their bill adjusted and their ESN/MIN changed. Further, cellular companies have started to install the latest in Inter-System PRV (Positive Roamer Validation). PRV signaling equipment

and SS-7 data links are now used to validate the identity and credit worthiness of roamers (those cellular users not operating in their subscriber territory) on the cellular network. Additionally, the cellular industry has taken to improved verification of credit information, address, identity checking, and roamer activity. Real time links to the credit bureaus for improved credit risk management has been initiated, as well as the calling of a subscriber's home or office to verify his billing address a few days after service has commenced.

Notwithstanding the cellular industry's extensive effort to stop the spread of cellular fraud, in the past, such pirates have been amazingly successful both in terms of speedy delivery to their markets and the magnitude of the stolen signals. In the coming decade, as the demand for cellular communications increases, signal theft is anticipated to increase at a rate at least comparable with increase of cellular communications.

Accordingly, their is a need to reduce the debt losses to the cellular industry, including direct losses from uncollected airtime revenues, increased expenses from interconnect charges from the need to hire extra staff to handle fraud problems on legitimate customers phones and monthly bills.

Further, their is a need to reduce the ability for organized criminals to operate using cellular phones.

Additionally, their is a need to reduce the inconvenience to legitimate cellular subscribers from wrong phone bills, strange incoming phone calls and the need to get their phone reprogrammed to a "clean" number.

For the foregoing reasons, there is a need to reduce or eliminate fraudulent use of a wireless system by improved detection and location of the fraudulent user. It would be desirable to verify if system users were authorized by virtue of their position.

Accordingly, it would be desirable if the cellular system would cease the transmission of signals to users determined to be fraudulent.

Additionally, it would be desirable to provide a cellular system that would provide for the apprehension of fraudulent users once their position had been determined.

SUMMARY OF THE INVENTION

The invention provides improvements in wireless communications systems. While various aspects of the invention will be explained by reference, for example, to a cellular communications system using spread spectrum waveforms, it will be apparent to those skilled in the art that these techniques are applicable to similar forms of wireless communications systems, such as, for example, Specialized Mobile Radio (SMR), the planned Personal Communications Service (PCS) and existing cellular radio systems.

The present invention is directed to improvements in such wireless communications systems, for example, a cellular communications system using spread spectrum waveforms. The spread spectrum system makes possible the use of very low rate, highly redundant coding without loss of capacity to accommodate a large number of users within the allocated bandwidth. Further, though not limited to such, the present invention is directed to a cellular communications using Code Division Multiple Access (CDMA) which is anticipated to have achieved world wide use in the coming decade.

Briefly, in one aspect, a wireless communication system of the present invention is directed to a wireless communications system which includes node means and a

plurality of user units, each said user unit including a means for establishing selective communication between the node means and the user unit. Such a system is improved by establishing the geographical location of a selected user. The geographical location of the selected user is compared to known locations of authorized users to determine if the communication system is being "pirated" and communication signals being fraudulently stolen. Once determination has been made that the selected user is an unauthorized recipient of the communications services, the cellular system can disrupt the communication services by numerous means. For example, in one embodiment of the present invention, the communication system disrupts communications services by simply ceasing the receipt or transmission of signals to the unauthorized selected user. In an additional embodiment, the nodal unit of the communications systems transmits a signal to the selected user instructing the user unit to disable itself. Though not intended to be limited thereto, this may be accomplished by scrambling the internal software of a user unit, instructing the user unit to destroy its internal circuitry or to blow an internal fuse.

In still another embodiment of the operation of the communications system, the determination of the geographical location of an unauthorized fraudulent user of the communication system provides means by which the

pirate may be apprehended and arrested. Once the position of the pirate is known, the information is forwarded to the police or other law enforcement agency such as the Federal Communications Commission (FCC). The law enforcement agency then proceeds to the geographic location, where the user unit is impounded and the pirate user is arrested. In this manner, not only is fraudulent use of the system reduced due to the arrest of those "pirating" the system, but those contemplating cellular theft are deterred from such actions due to the high risk of being apprehended.

As stated above, the present invention utilizes the knowledge of a users position to first verify the legitimate, authorized user units. The remaining units operating on that code are clearly identified as non-paying pirate users by having a different position. The communication system then operates to deny service to the selected user if the selected user's location does not correspond to one of the known locations of authorized users.

Preferably, the system includes means for determining the position of a selected user unit by providing a timing signal to the selected user unit from the node, providing a timing response signal from the selected user unit from the node, providing a time response signal from the selected user unit in response

to each timing signal, receiving the timing response signal by the node, measuring the response time of the user unit to the timing signal based on receipt of the timing response signal, and determining the position of the user unit based on the round trip time of transmission of the timing signal and receipt of the timing response signal.

In a more detailed aspect of the invention, the position means comprises means for measuring the response times of the user unit to respective timing signals transmitted by at least two nodes and for determining the position of the selected user unit based on the round trip times from each timing signal transmitting surface node.

In yet another aspect, the position means comprises means for determining the position of the selected user unit by measuring at a plurality of nodes the response time of the user unit to a timing signal transmitted by at least one of the nodes and determining the position of the selected user unit based on the times of receipt by the nodes of the timing response signal from the user unit.

In another aspect, the position means may store *a priori* information about the selected user unit and may determine the position of the selected user unit by

providing a timing signal to the user unit from a node, measuring the response time of the user unit to the timing signal at the node, and determining the position of the user unit based on such measurement and on the *a priori* information. Additionally, the position means also determines in which cell a selected user unit is and indicates the location of the cell.

Other aspects and advantages of the invention will become apparent from the following detailed description and the accompanying drawings, illustrating by way of example the features of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1(a)-(c) are diagrams showing an overview of the principal elements of typical communications systems which embody the principles of the invention;

FIG. 2 is a diagram of the frequency sub-bands of the frequency band allocation for a mobile system, e.g., a cellular system;

FIG. 3 is a block diagram of a satellite link system showing the user unit and satellite node control center;

FIG. 4 is a block diagram of one embodiment of a satellite signal processing in the system in FIG. 5;

FIG. 5 is a functional block diagram of a user transceiver;

FIG. 6 depicts the interrelationship of the cellular structure of the ground nodes, cellsite controller (CSC), and mobile switching center (MSC) of a typical system; and

FIG. 7 depicts an internal circuit of a user unit capable of being remotely operated to prevent further use of the user unit.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As is shown in the exemplary drawings, the invention is embodied in a mobile system, e.g., a cellular communications system utilizing integrated satellite and ground nodes both of which use the same modulation, coding, and spreading structure and both responding to an identical user unit.

Signal theft or "pirating" is a major problem in current cellular and TV receive only (TVRO) systems, and will probably affect additional future communications systems. Pirates manage to learn a code intended to restrict the system use to the authorized customers for whom it was intended, and then to alter users units such that they become pirate units which operate using the stolen code. Thus, unlawful use of the system is accomplished and the pirate user does not pay the fees due to the service provider. In the past, such pirates have been amazingly successful at their unlawful trade, both in terms of speedy delivery to their markets and the value of stolen signals. Such piracy continues on a large scale today not only in cellular communications systems but also other communications systems such as satellite television systems where satellite television transmissions are pirated.

This invention utilizes the knowledge of a users position, obtained as described above, first to verify the legitimate, authorized users unit. The remaining units operating on that code are clearly identified as non paying or pirate users by virtue of having a different position. In one embodiment, this information is used to apprehend the pirates.

In an alternate embodiment, the pirated unit can be disabled. There are two embodiments for disabling the pirated unit, each being effective under different circumstances. The first involves simply not providing service. The second involves commanding the disablement of the pirated unit by means including commanding that fuses to be blown within the circuitry and commanding the destruction of the user circuitry.

Referring now to FIG. 1(a), an overview of a typical communications system 10 is presented showing the functional inter-relationships of the major elements. The disclosed communication system is for example only and may be embodied in various forms. The system network control center 12 directs the top level allocation of calls to satellite and ground regional resources throughout the system. It also is used to coordinate system-wide operations, to keep track of user locations, to perform optimum allocation of system resources to each call, dispatch facility command codes, and monitor and

supervise overall system health. The regional node control centers 14, one of which is shown, are connected to the system network control center 12 and direct the allocation of calls to ground nodes within a major metropolitan region. The regional node control center 14 provides access to and from fixed land communication lines, such as commercial telephone systems known as the public switched telephone network (PSTN). The ground nodes 16 under direction of the respective regional node control center 14 receive calls over the fixed land line network, encode them, spread them according to the unique spreading code assigned to each designated user, combine them into a composite signal, modulate that composite signal onto the transmission carrier, and broadcast them over the cellular region covered.

Satellite node control centers 18 are also connected to the system network control center 12 via status and control land lines and similarly handle calls designated for satellite links such as from PSTN, encode them, spread them according to the unique spreading codes assigned to the designated users, and multiplex them with other similarly directed calls into an uplink trunk, which is beamed up to the designated satellite 20. Satellite nodes 20 receive the uplink trunks, frequency demultiplex the calls intended for different satellite cells, frequency translate and direct each to its appropriate cell transmitter and cell beam, and broadcast

the composite of all such similarly directed calls down to the intended satellite cellular area. As used herein, "backhaul" means the link between a satellite 20 and a satellite node control center 18. In one embodiment, it is a K-band frequency while the link between the satellite 20 and the user unit 22 uses an L-band or an S-band frequency.

As used herein, a "node" is a communication site or a communication relay site capable of direct one or two-way radio communication with users. Nodes may include moving or stationary surface sites or airborne or satellite sites.

User units 22 respond to signals of either satellite or ground node origin, receive the outbound composite signal, separate out the signal intended for that user by despreading using the user's assigned unique spreading code, de-modulate, and decode the information and deliver the call to the user. Such user units 22 may be mobile or may be fixed in position. Gateways 24 provide direct trunks that is, groups of channels, between satellite and the ground public switched telephone system or private trunk users. For example, a gateway may comprise a dedicated satellite terminal for use by a large company or other entity. In the embodiment of FIG. 1, the gateway 24 is also connected to that system network controller 12.

All of the above-discussed centers, nodes, units and gateways are full duplex transmit/receive performing the corresponding inbound (user to system) link functions as well in the inverse manner to the outbound (system to user) link functions just described.

FIGs. 1(b) and 1(c) represent systems with space only and ground only nodes. Certain aspects of this invention relate to these two systems as well as the "hybrid" system previously described.

Referring now to FIG. 2, the allocated frequency band 26 of a communications system is shown. The allocated frequency band 26 is divided into 2 main sub-bands, an outgoing sub-band 25 and an incoming sub-band 27. Additionally the main sub-bands are themselves divided into further sub-bands which are designated as follows:

OG: Outbound Ground 28 (ground node to user)
OS: Outbound Satellite 30 (satellite node to user)
OC: Outbound Calling and Command 32 (node to user)
IG: Inbound Ground 34 (user to ground node)
IS: Inbound Satellite 36 (user to satellite node)
IC: Inbound Calling and Tracking 38 (user to node)

All users in all cells use the entire designated sub-band for the described function. Unlike existing

ground or satellite mobile systems, there is no necessity for frequency division by cells; all cells may use these same basic six sub-bands. This arrangement results in a higher frequency reuse factor as is discussed in more detail below.

In one embodiment of the cellular system, a mobile user's unit 22 will send an occasional burst of an identification signal in the IC sub-band either in response to a poll or autonomously. This may occur when the unit 22 is in standby mode. This identification signal is tracked by the regional node control center 14 as long as the unit is within that respective region, otherwise the signal will be tracked by the satellite node or nodes. In another embodiment, this identification signal is tracked by all ground and satellite nodes capable of receiving it. This information is forwarded to the network control center 12 via status and command lines. By this means, the applicable regional node control center 14 and the system network control center 12 remain constantly aware of the cellular location and link options for each active user 22. An intra-regional call to or from a mobile user 22 will generally be handled solely by the respective regional node control center 14. Inter-regional calls are assigned to satellite or ground regional system resources by the system network control center 12 based on the location of the parties to the call, signal

quality on the various link options, resource availability and best utilization of resources.

A user 22 in standby mode constantly monitors the common outbound calling frequency sub-band OC 32 for calling signals addressed to him by means of his unique spreading code. Such calls may be originated from either ground or satellite nodes. Recognition of his unique call code initiates the user unit 22 ring function. When the user goes "off-hook", e.g., by lifting the handset from its cradle, a return signal is broadcast from the user unit 22 to any receiving node in the user calling frequency sub-band IC 38. This initiates a handshaking sequence between the calling node and the user unit which instructs the user unit whether to transition to either satellite, or ground frequency sub-bands, OS 30 and IS 36 or OG 28 and IG 34.

A mobile user wishing to place a call simply takes his unit 22 off hook and dials the number of the desired party, confirms the number and "sends" the call. Thereby an incoming call sequence is initiated in the IC sub-band 38. This call is generally heard by several ground and satellite nodes which forward call and signal quality reports to the appropriate system network control center 12 which in turn designates the call handling to a particular satellite node 20 or regional node control center 14. The call handling element then initiates a

handshaking function with the calling unit over the OC 32 and IC 38 sub-bands, leading finally to transition to the appropriate satellite or ground sub-bands for communication.

The combined satellite/ground nodes system provides a hierarchical geographical cellular structure. Thus within a dense metropolitan area, each satellite cell may further contain as many as 100 or more ground cells, which ground cells would normally carry the bulk of the traffic originated therein. The number of users of the ground nodes 16 is anticipated to exceed the number of users of the satellite nodes 20 where ground cells exist within satellite cells. Because all of these ground node users would otherwise interfere as background noise with the intended user-satellite links, in one embodiment the frequency band allocation may be separated into separate segments for the ground element and the space element as has been discussed in connection with FIG. 2. This combined, hybrid service can be provided in a manner that is smoothly transparent to the user. Calls will be allocated among all available ground and satellite resources in the most efficient manner by the system network control center 12.

Referring now to FIG. 3, a block diagram is shown of a typical user unit 22 to satellite 20 to satellite node control 18 communication and the processing involved in

the user unit 22 and the satellite node control 18. In placing a call for example, the handset 64 is lifted and the telephone number entered by the user. After confirming a display of the number dialed, the user pushes a "send" button, thus initiating a call request signal. This signal is processed through the transmitter processing circuitry 66 which includes spreading the signal using a calling spread code. The signal is radiated by the omni-directional antenna 68 and received by the satellite 20 through its narrow beamwidth antenna 62. The satellite processes the received signal as will be described below and sends the backhaul to the satellite node control center 18 by way of its backhaul antenna 70. On receive, the antenna 68 of the user unit 22 receives the signal and the receiver processor 72 processes the signal. Processing by the user unit 22 will be described in more detail below in reference to FIG. 5.

The satellite node control center 18 receives the signal at its antenna 71, applies it to a circulator 73, amplifies 74, frequency demultiplexes 76 the signal separating off the composite signal which includes the signal from the user shown in FIG. 3, splits it 78 off to one of a bank of code correlators, each of which comprises a mixer 80 for removing the spreading and identification codes, an AGC amplifier 82, the FECC demodulator 84, a demultiplexer 86 and finally a voice

encoder/decoder (CODEC) 88 for converting digital voice information into an analog voice signal. The voice signal is then routed to the appropriate land line, such as a commercial telephone system. Transmission by the satellite node control center 18 is essentially the reverse of the above described reception operation.

Referring now to FIG. 4, the satellite transponder 90 of FIG. 3 is shown in block diagram form. A circulator/diplexer 92 receives the uplink signal and applies it to an L-band or S-band amplifier 94 as appropriate. The signals from the M satellite cells within a "cluster" are frequency multiplexed 96 into a single composite K-band backhaul signal occupying M times the bandwidth of an individual L-/S-band mobile link channel. The composite signal is then split 98 into N parts, separately amplified 100, and beamed through a second circulator 102 to N separate satellite ground cells. This general configuration supports a number of particular configurations various of which may be best adapted to one or another situation depending on system optimization which for example may include considerations related to regional land line long distance rate structure, frequency allocation and subscriber population. Thus, for a low density rural area, one may utilize an M-to-1 (M>1, N=1) cluster configuration of M contiguous cells served by a single common satellite ground node with M limited by available bandwidth. In

order to provide high-value, long distance service between metropolitan area, already or best covered for local calling by ground cellular technology, an M-to-M configuration would provide an "inter-metropolitan bus" which would tie together all occupants of such M satellite cells as if in a single local calling region. To illustrate, the same cells (for example, Seattle, Los Angeles, Omaha and others) comprising the cluster of M user cells on the left side of FIG. 4, are each served by corresponding backhaul beams on the right side of FIG. 4.

Referring now to FIG. 5, a functional block diagram of a typical user unit 22 is shown. The user unit 22 comprises a small, light-weight, low-cost, mobile transceiver handset with a small, non-directional antenna 68. The single antenna 68 provides both transmit and receive functions by the use of a circulator/diplexer 104 or other means. It is fully portable and whether stationary or in motion, permits access to a wide range of communication services from one telephone with one call number. It is anticipated that user units will transmit and receive on frequencies in the 1-3 GHz band but can operate in other bands as well.

The user unit 22 shown in FIG. 5 comprises a transmitter section 106 and a receiver station 108. For the transmission of a voice communication, a microphone couples the voice signal to a voice encode 110 which

performs analog to digital encoding using one of the various modern speech coding technologies well known to those skilled in the art. The digital voice signal is combined with local status data, and/or other data, facsimile, or video data forming a composite bit stream in digital multiplexer 112. The resulting digital bit stream proceeds sequentially through forward error encoder 114, symbol or bit interleaver 116, symbol or bit, phase, and/or amplitude modulator 118, narrow band IF amplifier 120, wideband multiplier or spreader 122, wide band IF amplifier 124, wide band mixer 126, and final power amplifier 128. Oscillators or equivalent synthesizers derive the bit or baud frequency 130, pseudo-random noise or "chip" frequency 132, and carrier frequency 134. The PRN generator 136 comprises deterministic logic generating a pseudo-random digital bit stream capable of being replicated at the remote receiver. The ring generator 138 on command generates a short pseudo-random sequence functionally equivalent to a "ring".

The transceiver receive function 108 demodulation operations mirror the corresponding transmit modulation functions in the transmitter section 106. The signal is received by the non-directional antenna 68 and conducted to the circulator 104. An amplifier 142 amplifies the received signal for mixing to an IF at mixer 144. The IF signal is amplified 146 and multiplied or despread 148

and then IF amplified 150 again. The IF signal then is conducted to a bit or symbol detector 152 which decides the polarity or value of each channel bit or symbol, a bit or symbol de-interleaver 154 and then to a forward error decoder 156, the composite bit stream from the FEC decoder 156 is then split into its several voice, data, and command components in the de-multiplexer 158. Finally a voice decoder 160 performs digital to analog converting and results in a voice signal for communication to the user by a speaker or other means. Local oscillator 162 provides the first mixer 144 LO and the bit or symbol detector 152 timing. A PRN oscillator 164 and PRN generator 166 provide the deterministic logic of the spread signal for despreading purposes. The baud or bit clock oscillator 168 drives the bit in the bit detector 152, forward error decoder 156 and the voice decoder 160.

The bit or symbol interleaver 116 and de-interleaver 154 provide a type of coded time diversity reception which provides an effective power gain against multipath fading to be expected for mobile users. Its function is to spread or diffuse the effect of short burst of channel bit or symbol errors so that they can more readily be corrected by the error correction code.

As an alternative mode of operation, provision is made for direct data or facsimile or other digital data

input 170 to the transmitter chain and output 172 form the receiver chain.

A command decoder 174 and command logic element 176 are coupled to the forward error decoder 156 for receiving commands or information. By means of special coding techniques known to those skilled in the art, the non-voice signal output at the forward error decoder 156 may be ignored by the voice decoder 160 but used by the command decoder 174. An example of the special coding techniques are illustrated in FIG. 5 by the MUX 112 and DEMUX 158.

As shown, acquisition, control and tracking circuitry 178 are provided in the receiver section 108 for the three receive side functional oscillators 162, 164, 168 to acquire and track the phase of their counterpart oscillators in the received signal. Means for so doing are well known to those skilled in the art.

Referring again to FIG. 5, an arrangement is provided for generating call requests and detecting ring signals. The ring generator 138 generates a ring signal based on the user's code for calling out with the user unit 22. For receiving a call, the ring signal is detected in a fixed matched filter 198 matched to a short pulse sequence which carries the user's unique code. By this means each user can be selectively called. As an

option, the ring detect and call request signals may be utilized in poll/response mode to provide tracking information on each active or standby mode user. Course tracking information, adequate for management of the call routing functions is provided by comparison of signal quality as received at various modes.

With reference also to FIG. 6, for the precision location option, the user response signal time is accurately locked to the time of receipt of the polling or timing signal, to a fraction of a PRN chip width. Measurement of the round trip poll/response time from two or more nodes or time differences of arrival at several nodes provides the basic measurement that enable solution and provision of precise user position. Ground and satellite transmitters and receivers duplicate the functions summarized above for the user units. Given *a priori* information, for example as to the route plan of a vehicle, a single round trip poll/response time measurement from a single node can yield valuable user position information.

The command logic 176 is further coupled to the receiver AGC 180, the matched filter ring detector (RD) 198, the acquisition and tracking circuitry 178, the transmit local oscillator (LO) 162 and the ring generator (RG) 138 to command various modes of operation.

A preferred communication system includes the use of spread spectrum multiple access so that adjacent cells are not required to use different frequency bands. All ground-user links utilize the same two frequency sub-bands (OG 28, IG 34) and all satellite-user links use the same two frequency sub-bands (OS 30, IS 36). This obviates an otherwise complex and restrictive frequency coordination problem of ensuring that frequencies are not reused within cells closer than some minimum distance to one another (as in the FM approach), and yet provides for a hierarchial set of cell sizes to accommodate areas of significantly different subscriber densities.

The economic feasibility of a mobile telephone system is related to the number of users that can be supported. Two significant limits on the number of users supported are bandwidth utilization efficiency and power efficiency. In regard to bandwidth utilization efficiency, in either the ground based cellular or mobile satellite elements, radio frequency spectrum allocation is a severely limited commodity. Measures incorporated in the invention to maximize bandwidth utilization efficiency include the use of code division multiple access (CDMA) technology which provides an important spectral utilization efficiency gain and higher spatial frequency reuse factor made possible by the user of smaller satellite antenna beams. In regard to power efficiency, which is a major factor for the satellite-

mobile links, the satellite transmitter source power per user is minimized by the use of forward-error-correcting coding, which in turn is enabled by the above use of spread spectrum code division multiple access (SS/CDMA) technology and by the use of relatively high antenna gain on the satellite. CDMA and forward-error-correction coding are known to those skilled in the art and no further details are given here.

One aspect of the invention is directed to accurate position determination of individual users of the cellular communications system.

With reference to FIG. 6, a cellular system is disclosed having a plurality of cellular nodes, 400, 402, 404, 406, 408, 410, and 412, respectively, forming cellular sectors 414, 416, 418, 420, 422, 424, and 426, respectively. Controlling receipt and transmission of signals is the cellsite controller (CSC) 430 and the mobile switching center (MSC) 432. It is anticipated for the cellular system to include a plurality of user units. However, a single user unit 440 is shown for example only.

For precision location of the user, the user response signal time is accurately locked to the time of receipt of the polling or timing signal, to a fraction of a PRN chip width. The distance between an individual

node and a user may then be determined by providing a timing signal to the selected user unit from at least one node, providing a timing response signal from the selected user unit in response to each timing signal, receiving the timing response signal by at least one node, and measuring the response time of the user unit to the timing signal. The position of the user unit can then be determined based on the round trip time of transmission of the timing signal and receipt of the timing response signal from a plurality of nodes. Measurement of the round trip poll/response time from two or more nodes or time differences of arrival at several nodes provides the basic measurement that enables solution and provision of precise user position. For example, round trip poll/response times from nodes 400, 402, and 406 to user unit 440 provides the measurement of distances 450, 452, and 454. Through simple analysis, or alternatively, use of a Kalman filter, the central cellsite controller can determine the location of the user unit.

In another aspect of the invention, given *a priori* information, for example, as to the route plan of a vehicle, a single round trip poll/response time measurement from a single node can yield valuable user position information. The position means may store *a priori* information about the selected user unit and may determine the position of the selected user unit by

providing a timing signal to the user unit from a node, measuring the response time of the user unit to the timing signal at the node, and determining the position of the user unit based on such measurement and on the *a priori* information. An example of *a priori* information includes the sought to be travelled route of a user. By knowing the route of a selected user and the distance from a node, determined by application of the present invention, the central controller can determine the position of a selected user.

In another embodiment of position determination including the use of *a priori* information, the position of the user unit can be determined by distance determination from only two nodes. For example, the distances 452 and 454 of user unit 440 from nodes 402 and 406 combined the *a priori* information that the user unit is located cell sector 414 provides the necessary information to accurately determine the location of user unit 440. This *a priori* information may be determined by knowledge of the user unit's last known location or by analysis of the signal quality of the user unit's transmissions by cell nodes 400, 402, 404 and 406 to determine the user unit's location to be in cell sector 414. In another embodiment, once the user unit's location and present cell cite has been determined utilizing the three node trigonometric analysis described above, the cell site controller may switch to two node

position determination thereby reducing computer computations.

Ideally suited for position determination is the use of code division multiple access (CDMA) technology which provides an important spectral utilization efficiency gain and higher spatial frequency reuse factor made possible by the use of smaller satellite antenna beams. In regard to power efficiency, which is a major factor for the satellite-mobile links, the satellite transmitter source power per user is minimized by the use of forward-error-correcting coding, which in turn is enabled by the above use of spread spectrum code division multiple access (SS/CDMA) technology and by the use of relatively high antenna gain on the satellite. CDMA and forward-error-correction coding are known to those skilled in the art and no further details are given here.

In addition, the Code Division Multiplex system has the following important advantages in the present system. Blank time when some of the channels are not in use reduces the average interference background. In other words, the system overloads and underloads gracefully. The system inherently provides flexibility of base band rates; as opposed to FDM systems, signals having different baseband rates can be multiplexed together on an ad-hoc basis without complex preplanned and restrictive sub-band allocation plans. Not all users

need the same baseband rate. Satellite antenna sidelobe control problems are significantly reduced. Numerical studies of out-of-cell interference factors show that secondary lobe responses may effectively be ignored. Co-code reassignment (that is reuse of the same spreading code) is feasible with just one beam separation. However, because there are effectively (i.e. including phasing as a means of providing independent codes) an unlimited number of channel codes, the requirements on space division are eased; there is no need to reuse the same channel access i.e., spreading code.

Accurate position determination can be obtained through two-dimensional multi-lateration. Each CDMA mobile user unit's transmitted spreading code is synchronized to the epoch of reception of the pilot signal from its current control site, whether ground or satellite node. The normal mode of operation will be two-dimensional, i.e., based upon two receptions, at ground or satellite nodes of the user response code. In conjunction with *a priori* information inherent in a topographic database, e.g., altitude of the surface of the earth, position accuracy to within a fraction of a kilometer can be provided.

In a CDMA system, means for determining the position of a mobile user relative to a multiplicity of known system nodes, either fixed on the ground or at known

positions in space, is largely incidental to the function of transmitting and/or receiving the CDMA signal at multiple sites. The receiving function requires synchronization of the epoch of a local spread code generator to that of the received spread code, so that having achieved code synchronization, one inherently has a measure of the delay time and hence the range of the signal. Various references describe how this information can be used in several different geometrical configurations to provide the delay measurements necessary to provide hyperbolic, elliptical, spherical or hybrid multi-lateration position determination. By any of these means the mobile position can either be determined by the network controller or by the mobile user and relayed to the network controller.

An additional aspect of the present invention is the determination of a fraudulent user by analysis of the position of a user in the system. The position of all users is periodically determined by the network controller. In one aspect of the invention, the controller is programmed to search for the same user ID appearing at locations which could not possibly be reached by the same user. A determination by the cellsite controller indicating that two or more units utilizing the same ESN/MIN, though not operating contemporaneously, have been operating in locations which could have been reached by a single user unit establishes

that there are one or more pirated units in use.

In one embodiment, the computer software keeps track of each user's position in the system and the time period and location between uses of the system.

An algorithm determines whether any two or more uses could not have been made by a single user. For example only, algorithm (A) may equal the distance between the location of the last known transmission and present transmission divided by the time differences between the last positions.

$$A = \frac{\text{(distance of previous and present uses)}}{\text{(time period between transmissions)}}$$

If the result exceeds, say, 100 MPH for any pair of transmissions, one or more separate users of the same ID code are indicated. Only one will be a valid user, the others will be "Bandits" (typically there will be many such "Bandits"). To determine the legitimate user, the user nearest the home address of the valid subscriber will be queried to determine whether or not that caller is a valid subscriber. The query can be either human to human, or machine to machine. If the first such queried party is legitimate, he is assigned a new ESN/MIN

combination, and the prior code is placed in a category recognized by the network controller as invalid. All the bandit users are then operating using an invalid code, and the next steps will be determined by the current service owner's policy and will include (a) causing the Bandits to be pursued for theft, (b) causing the bandit units to be disables or (c) ceasing service to these units as discussed below.

If the first such queried party is not legitimate the next party will be queried until the valid party is determined. If the distance between tracks is greater than 100 miles, then all users are queried, again beginning with the user nearest to the home address of the legitimate party, until the legitimate user is found. All other users are then Bandits, and are treated as below.

In an alternative embodiment, the cellsite controller initiates separate algorithms dependent upon the distance between transmissions. For example, the constant "A" in the equation:

$$A = \frac{\text{(distance of previous and present uses)}}{\text{(time period between transmissions)}}$$

may be altered where the distance between the previous use and the present use of the cellular system is greater

than 100 miles. In this manner, the cellular system is capable of compensating for those instances where a legitimate subscriber has travelled by plane to a new location. Further, a series of algorithms may be employed depending upon the various distances between transmissions and different periods between transmissions to account for common user habits and local topography, e.g. urban vs. rural travel. Such algorithms and the methods for creating such are known to those skilled in the art and no further details are given here.

An additional aspect of the present invention is that once a unit has been determined to be a fraudulently operated unit, (a) the bandit is pursued for theft, (b) the bandit unit is caused to be disabled or (c) service to the user unit is ceased. In a first embodiment, the cellular system merely ceases to provide service to anyone using the ESN/MIN combination determined to have been pirated.

The counterfeited ESN/MIN combination is denied service and the bandit is no longer capable engaging the cellular system without obtaining an alternative authorized ESN/MIN combination. Additionally, the valid subscriber is also denied service and must have his MIN (cellular telephone number) changed in order to have his service restored.

In an alternative embodiment, the cellsite controller transmits a remote erasure or alteration signal from the Cellular Node to the bandit user unit to erase or alter the mobile phone's operating software.

If fraud has been detected by the cellular system on a particular MIN/ESN combination, then the cellular node sends a pre-determined registration or call origination page message to the counterfeited phone. This pre-determined message instructs the phone to activate a self-destructing software algorithm which erases, scrambles or otherwise alters the phone's stored operating program in E^2PROM as well as the phone's Electronic Serial Number, Mobile Identification Number, Station Class Mark, etc., so that it is now rendered completely useless to the counterfeiter.

If the phone is in a call mode when the cellular switch wishes to deactivate it, then the "self-destruct algorithm" could also be activated by having the cellular node send either a pre-determined dual tone multiple frequency (DTMF) or Forward Voice Channel signaling message to it. This program and memory altering algorithm could be stored in the phone as a hidden "virus" which is activated only upon a certain code being transmitted to the phone, but otherwise is not easily detectable in the phone's software. For example, the hidden "virus" may be disguised as another piece of the

phone's normal operating code. In this form of counterfeiting countermeasure, the unit is disabled remotely rendering the keyboard and display inactive, such that none of the keys operate on the mobile unit's keypad and signals can be neither transmitted nor received. Alternatively, the user unit displays an error message indicating to the subscriber that he needs to get his unit examined by an authorized service center. In order to get the unit operating again the counterfeiter would need to replace the unit's software at an authorized dealer or service center making possible the impounding of the counterfeit unit and the apprehension of the bandit.

In another embodiment, once a cellular ESN/MIN has been identified by the cellular operator as being counterfeit, the MIN is place into a "customer group" which routes all its outgoing calls to a recorded message, instructing the authorized subscriber to have his unit re-programmed at an authorized dealer. Once the real subscriber has had his identity verified and his user unit reprogrammed, the ESN/MIN combination is deactivated from the cellular system, so that the counterfeit unit is unable to make calls.

In an additional embodiment, the cell site controller sends a disablement signal, operating to physically damage one or more critical components of the

user unit. For example, the user unit is disabled by having one or more of its components destroyed by commanding an increase of current in a certain path which blows a fuse or critical component. With reference to FIG. 7, an electronic switch 464 is commanded to be closed by a signal transmitted from the cellular node. The voltage differential between Vcc 466 and 0v 468 provides a current that is switched from the circuit path through resistor 462 to a short through electrical switch 464. The current passing through critical component 460 is thereby increased to a level where the component, such as a fuse, is damaged. Thus, once the counterfeiting of a user unit is detected, the switch is closed by remote control and the critical phone component is destroyed by the increased current flowing through it. The phone is rendered inoperable and has to be repaired by the authorized service center. An attempted repair of the damaged user unit also makes possible the impounding of the counterfeit unit and the apprehension of the bandit.

In still another embodiment, the determination of the geographical location of an unauthorized user provides means by which the pirate may be apprehended and arrested. Once the position of the pirate is known, the information is forwarded to the police or other law enforcement agency such as the Federal Communications Commission (FCC). The law enforcement agency then proceeds to the geographic location of the bandit where

the user unit is impounded and the bandit is arrested.

By virtue of the above discussed design factors the system in accordance with the invention provides a flexible capability of providing the following services: high quality, high rate voice and data service; facsimile (the standard group 3 as well as the high speed group 4); two way messaging, i.e. data interchange between mobile terminals at variable rates; paging rural residential telephone; private wireless exchange; automatic position determination and reporting to within several hundred feet, in conjunction with fraudulent detection of unauthorized users and the prevention thereof.

By virtue of the above discussed design factors the system in accordance with the invention provides a flexible capability of providing the following additional special services: high quality, high rate voice and data service; facsimile (the standard group 3 as well as the high speed group 4); two way messaging, i.e., data interchange between mobile terminals at variable rates; automatic position determination and reporting to within several hundred feet; paging rural residential telephone; and private wireless exchange.

It is anticipated that a satellite will utilize geostationary orbits but is not restricted to such. The invention permits operating in other orbits as well. The

system network control center 12 is designed to normally make the choice of which satellite or ground node a user will communicate with. In another embodiment, as an option, the user can request his choice between satellite link or direct ground based link depending on which provides clearer communications at the time or request his choice based on other communication requirements.

While a satellite node has been described above, it is not intended that this be the only means of providing above-ground service. In the case where a satellite has failed or is unable to provide the desired level of service for other reasons, for example, the satellite has been jammed by a hostile entity, an aircraft or other super-surface vehicle may be commissioned to provide the satellite functions described above. The "surface" nodes described above may be located on the ground or in water bodies on the surface of the earth. Additionally, while users have been shown and described as being located in automobiles, other users may exist. For example a satellite may be a user of the system for communicating signals, just as a ship at sea may or a user on foot.

While several particular forms of the invention have been illustrated and described, it will be apparent that various modifications can be made without departing from the spirit and scope of the invention. For example, the present invention is not meant to be limited to cellular

mobile communications systems but is intended to include additional communication systems, such as satellite or nodal television systems such as the recently marketed "Direct TV" system. Accordingly, it is not intended that the invention be limited, except by the appended claims.

Having described the invention in such terms as to enable those skilled in the art to make and use it, and having identified the presently preferred best modes thereof, I claim:

1. A communications system having a plurality of user units and at least one cellular node so as to establish at least one cell, the cellular communications system comprising:

a) position determination means for establishing the geographical location of a selected user;

b) logic means for comparing the location of said selected user with the known locations of authorized users; and

c) fraudulent detection means for determining whether said selected user is a fraudulent user of the communications system.

2. The communications system of claim 1, further comprises:

a) disablement means for denying service to said selected user if said selected user is a fraudulent user of the communications system.

3. The communications system of claim 2, wherein:

a) said disablement means includes a commanding means for sending a signal to said user unit to disable operation of said user unit.

4. The communications system of claim 3, wherein:

a) said commanding means is capable of destroying critical components in the user unit.

5. The communications system of claim 1, wherein:

a) said position means for determining the geographic location of a selected user unit is determined by providing a timing signal to the user unit from one or more nodes, providing a timing response signal from the selected user unit in response to each timing signal, receiving the timing response signal by at least one node, measuring the response time of the user unit to each timing signal, and determining the position of the user unit based on such measurements.

6. In the operation of a communications system, which system includes node means, and a plurality of user units, each said user unit including means for establishing selective communication between the node means and the user unit, the improvement for reducing use of said system by an unauthorized user, comprising:

a) establishing the geographical location of a selected user;

b) comparing the location of said selected user with the known locations of authorized users; and

c) determining whether said selected user is a fraudulent user based upon the comparison of the location of said selected user with the known locations of authorized users.

7. In the operation of a system of claim 6, further comprising:

a) denying service to said selected user if said selected user's location does not correspond to one of said known locations.

8. In the operation of a system of claim 6, further comprising:

a) apprehending said selected user.

9. In the operation of a system of claim 6, further comprising:

a) disabling said user unit.

10. In the operation of a system of claim 9, further comprising:

a) destroying a critical component in said user unit.

11. In the operation of a system of claim 6, wherein establishing the geographical location of a selected user further comprises:

a) providing a timing signal to said selected user unit from at least one node;

b) providing a timing response signal from the selected user unit in response to the timing signal;

c) receiving the timing response signal by at least one node;

d) measuring the response time of the user unit to the timing signal based on receipt of the timing response signal; and

e) determining the position of the user unit based on the round trip time of transmission of the timing signal and receipt of the timing response signal.

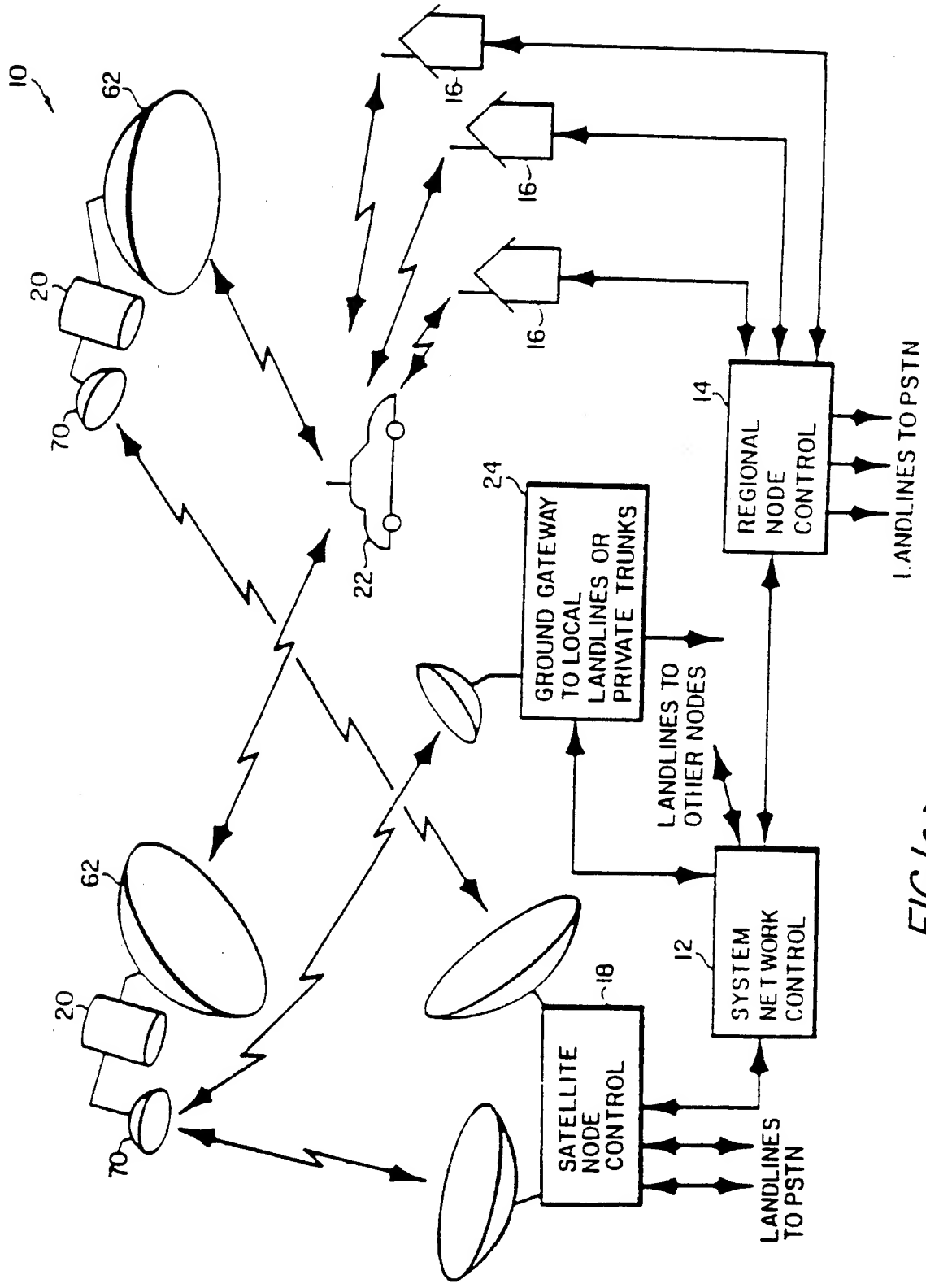

10
62
20
70
16
16
16
22
24
GROUND GATEWAY TO LOCAL LANDLINES OR PRIVATE TRUNKS
14
REGIONAL NODE CONTROL
LANDLINES TO PSTN
LANDLINES TO OTHER NODES
62
20
70
18
SATELLITE NODE CONTROL
12
SYSTEM NETWORK CONTROL
LANDLINES TO PSTN

FIG. 1(a)

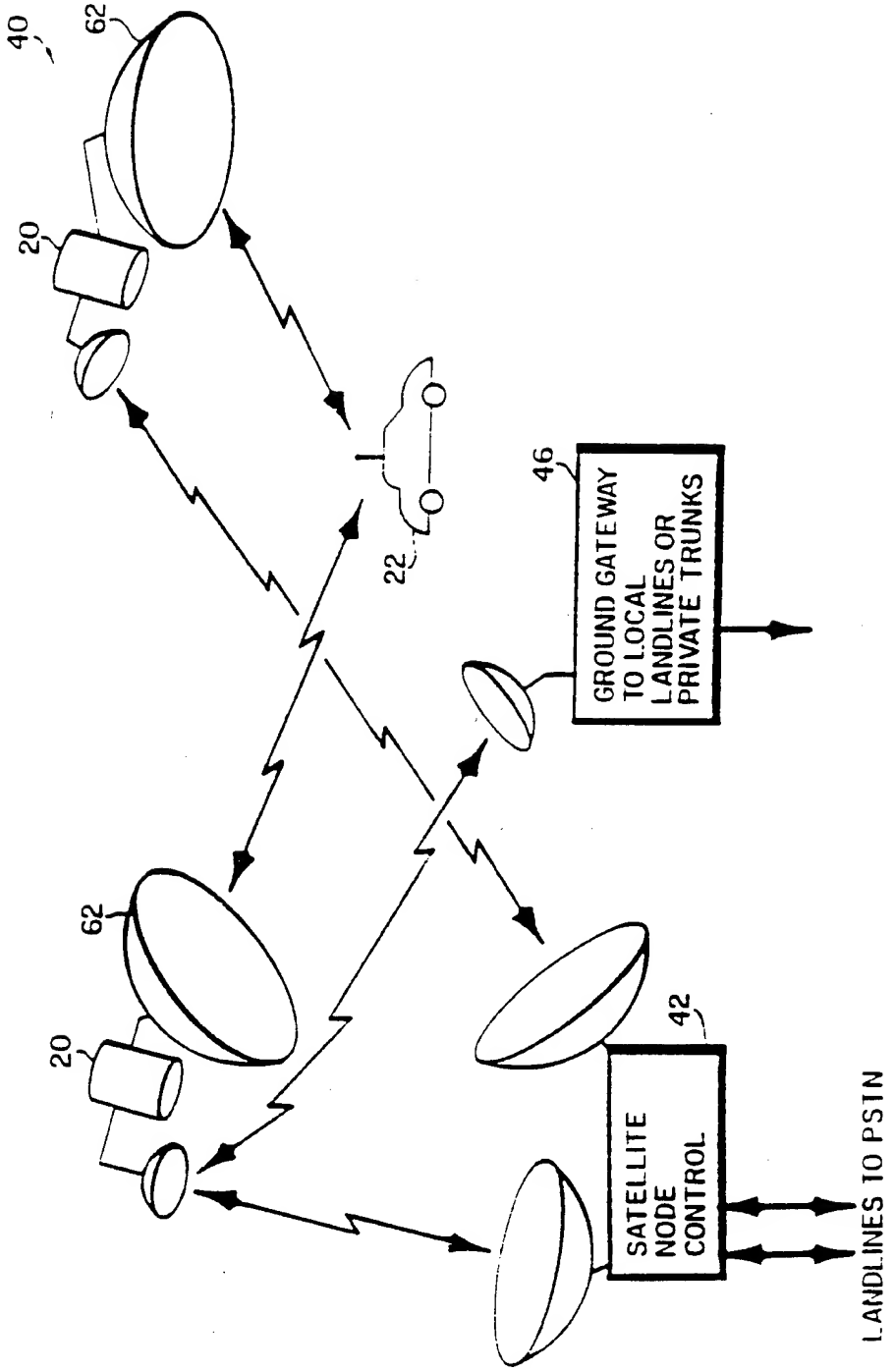

40
62
20
22
46
GROUND GATEWAY TO LOCAL LANDLINES OR PRIVATE TRUNKS
62
20
42
SATELLITE NODE CONTROL
LANDLINES TO PSTN

FIG. 1(b)

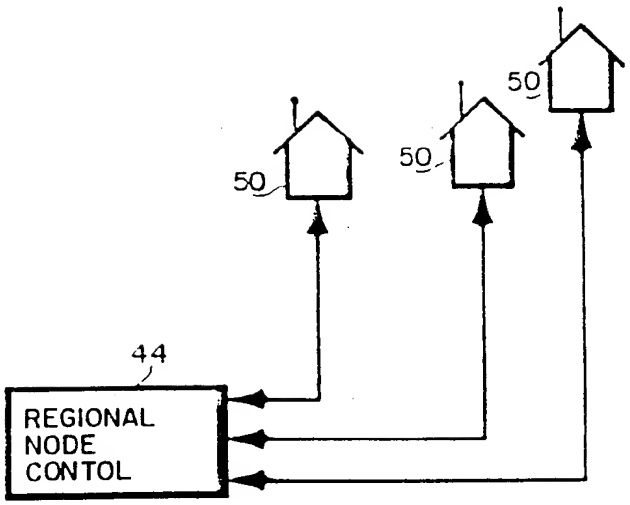


FIG. 1(c)

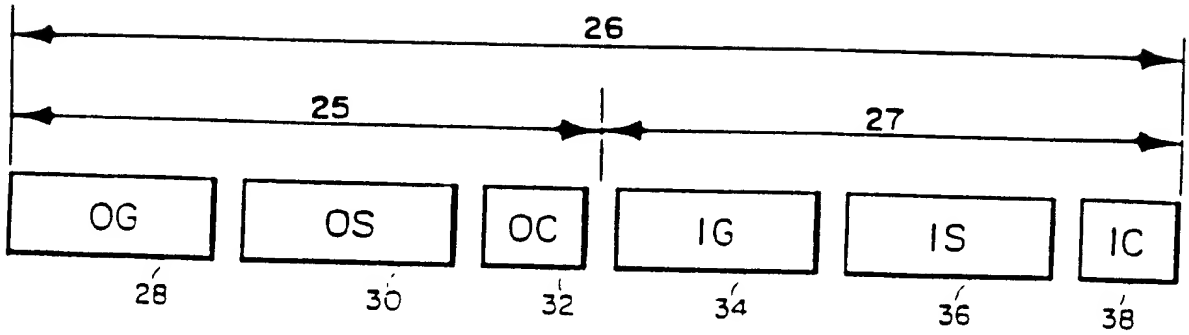


FIG. 2

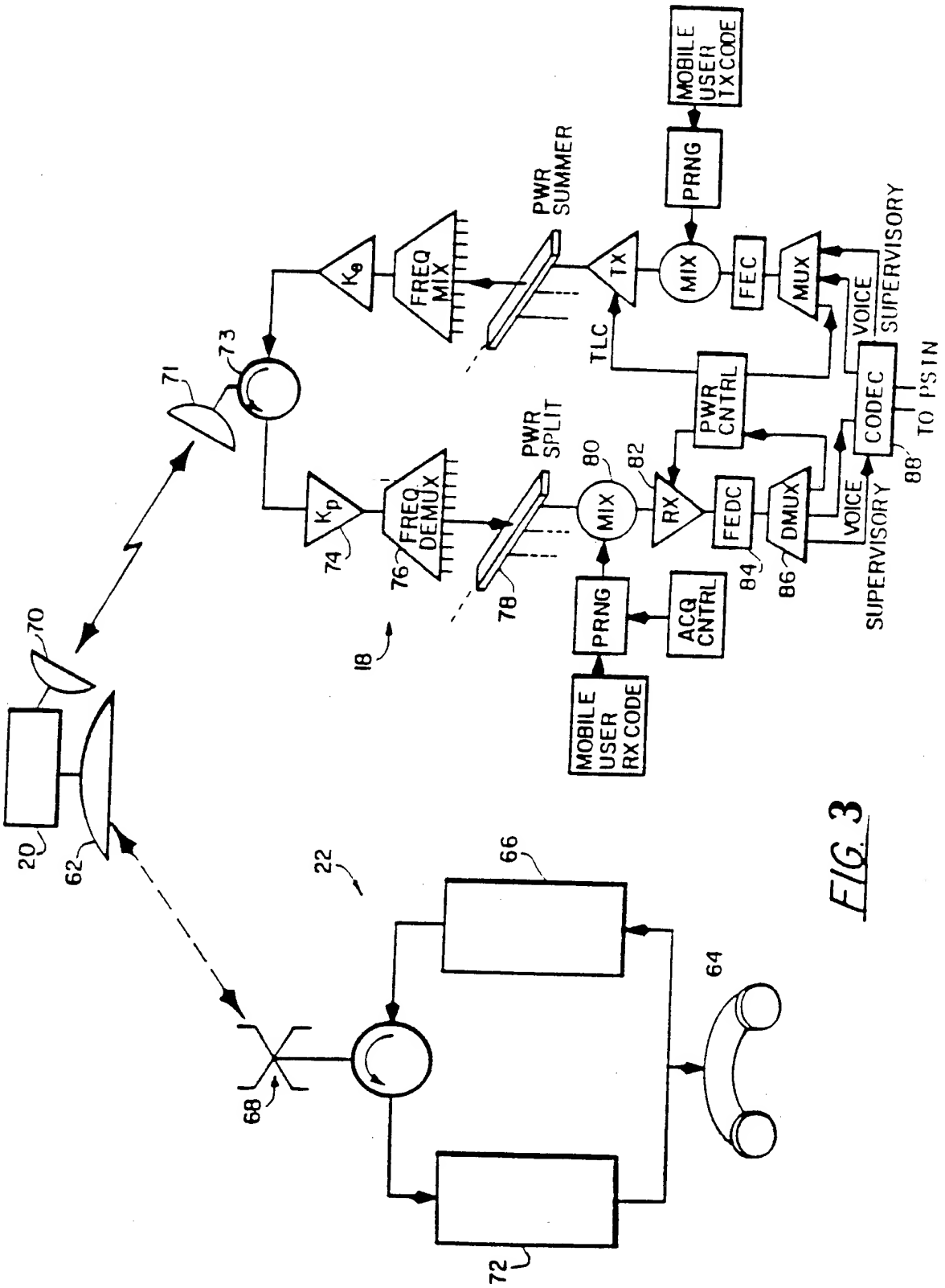

MOBILE USER TX CODE
PRNG
PWR SUMMER
K_e
FREQ MIX
TX
MIX
FEC
MUX
VOICE
SUPERVISORY
TLC
PWR CNTRL
CODEC
TO PSTN
88
73
71
PWR SPLIT
80
82
K_p
FREQ DEMUX
74
76
78
MIX
RX
FEDC
DMUX
84
86
VOICE
SUPERVISORY
18
PRNG
ACQ CNTRL
MOBILE USER RX CODE
70
20
62
22
66
64
68
72

FIG. 3

WO 95/34177 PCT/US95/07251

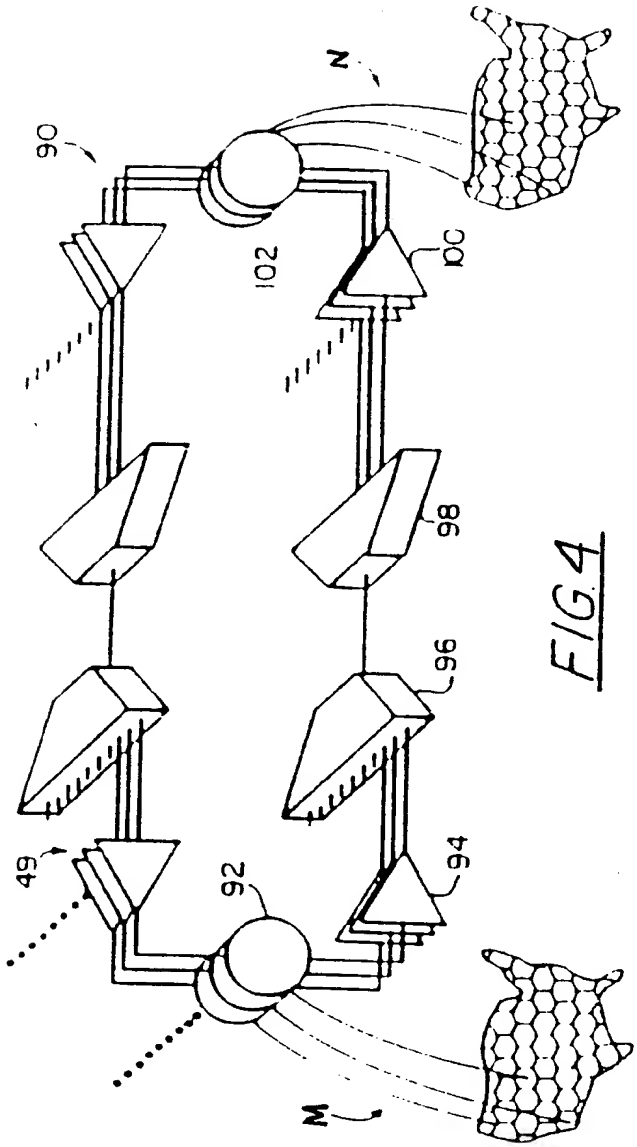
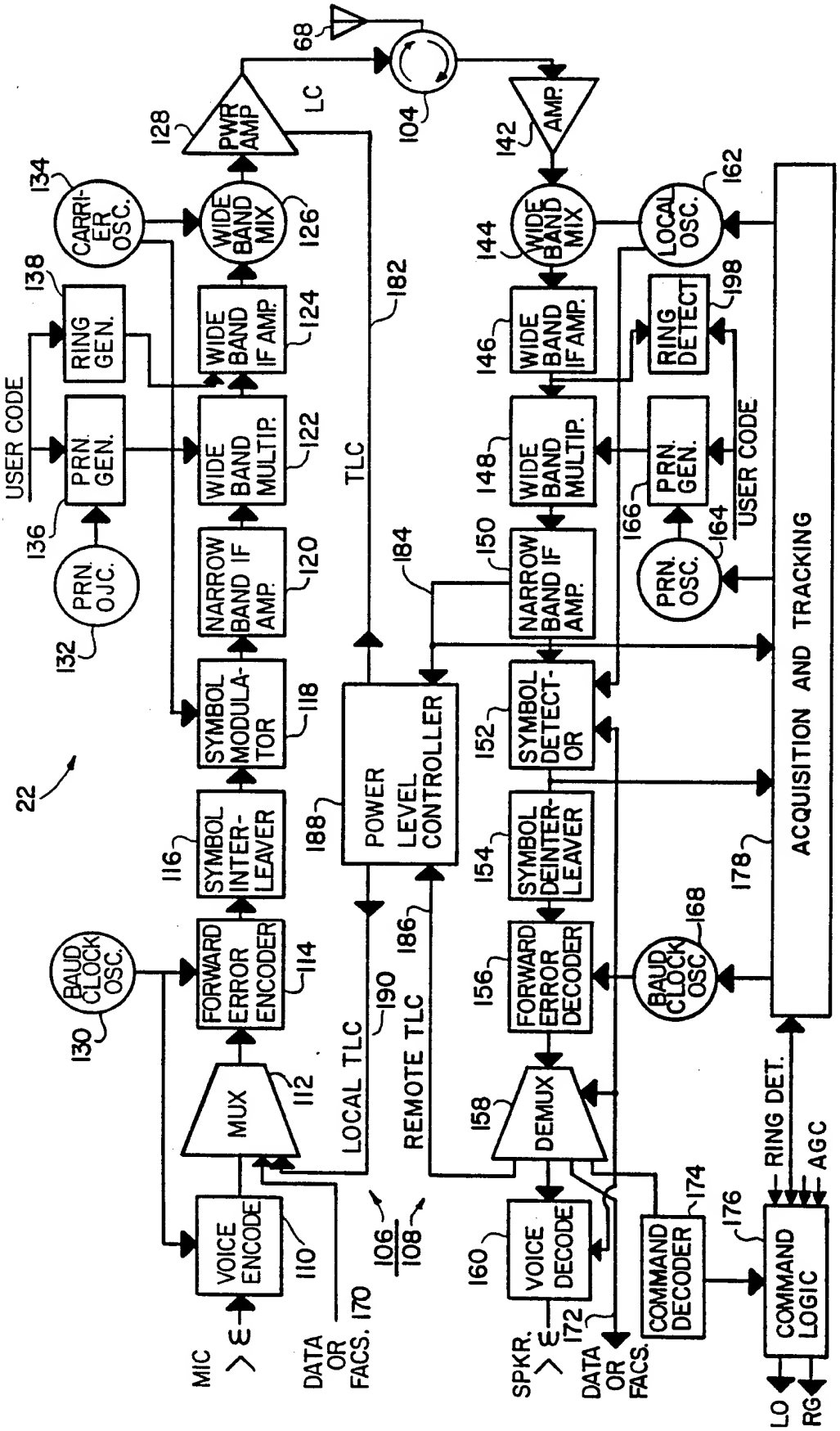


FIG 4

FIG. 5


22
68
104
LC
128
PWR AMP
142
AMP.
134
CARRIER OSC.
WIDE BAND MIX
126
144
WIDE BAND MIX
LOCAL OSC.
162
138
RING GEN.
WIDE BAND IF AMP.
124
146
WIDE BAND IF AMP.
RING DETECT
198
USER CODE
PRN. GEN.
136
WIDE BAND MULTIP.
122
148
WIDE BAND MULTIP.
PRN. GEN.
166
USER CODE
182
TLC
PRN. OJC.
132
NARROW BAND IF AMP.
120
184
150
NARROW BAND IF AMP.
PRN. OSC.
164
ACQUISITION AND TRACKING
SYMBOL MODULA-TOR
118
POWER LEVEL CONTROLLER
188
152
SYMBOL DETECT-OR
116
SYMBOL INTER-LEAVER
154
SYMBOL DEINTER-LEAVER
178
BAUD CLOCK OSC.
130
FORWARD ERROR ENCODER
114
186
156
FORWARD ERROR DECODER
BAUD CLOCK OSC.
168
MUX
112
LOCAL TLC
190
REMOTE TLC
158
DEMUX
RING DET.
AGC
106
108
VOICE ENCODE
110
160
VOICE DECODE
COMMAND DECODER
174
176
COMMAND LOGIC
MIC
DATA OR FACS.
170
SPKR.
172
DATA OR FACS.
LO
RG

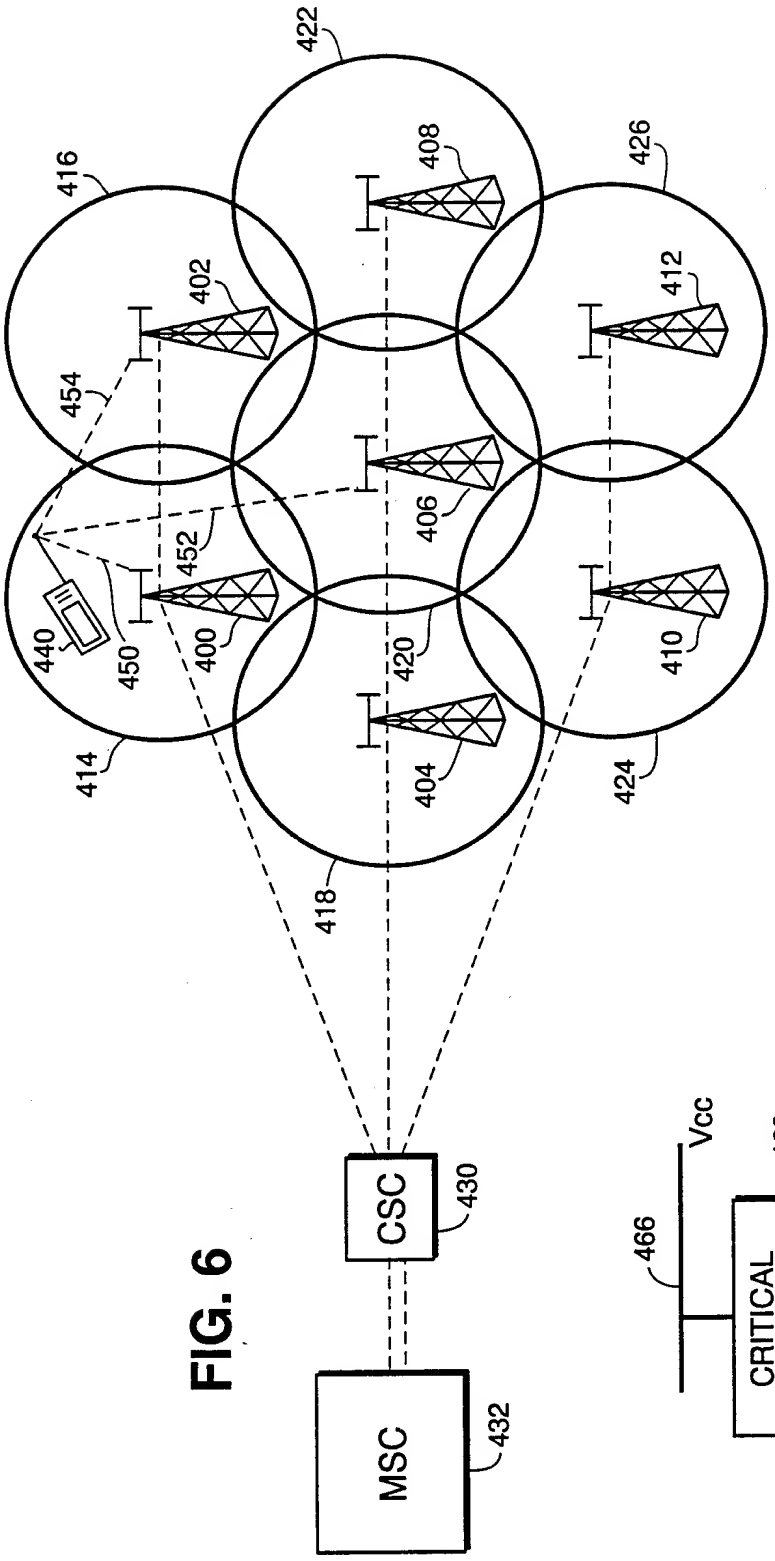

422
416
408
426
402
412
454
406
452
440
450
400
420
410
414
404
424
418
CSC
430
MSC
432

FIG. 6

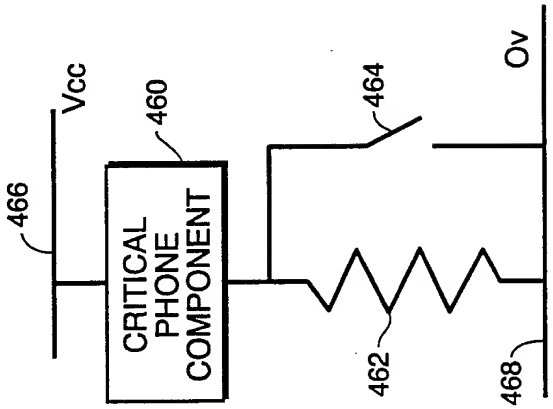

Vcc
460
464
Ov
466
CRITICAL PHONE COMPONENT
462
468

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/07251

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04Q 7/20
US CL :455/33.1, 54.1, 67.1; 379/59
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : Please See Extra Sheet.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P ------- Y,P	US, A, 5,335,265 (COOPER ET AL) 02 August 1994, abstract, col. 1, lines 51-58, col. 2, lines 6-26, col. 5, lines 8-14, col. 8, lines 26-68, col. 9, lines 1-14.	1-4, 6-10 ---------- 5, 11
Y	US, A, 4,278,975 (KIMURA ET AL) 14 July 1981, col. 4, lines 3-12.	5, 11
X,P ------- Y,P	US, A, 5,345,595 (JOHNSON ET AL) 06 September 1994, col. 3, lines 42-68, col. 13, lines 45-55.	1, 6 ---------- 2-5, 7-11
Y,P	US, A, 5,420,910 (RUDOKAS ET AL) 30 May 1995, col. 2, lines 13-41.	2-4, 7-10

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 AUGUST 1995	01 SEP 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20[illegible] Facsimile No. (703) [illegible]05-3230	Authorized officer NGUYEN VO Telephone No. (703) 308-6728

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/07251

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US, A, 5,335,278 (MATCHETT ET AL) 02 August 1994, col. 1-4.	1-11
A	US, A, 5,309,501 (KOZIK ET AL) 03 May 1994, col. 1-2.	1-11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/07251

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

455/33.1, 54.1, 67.1, 33.2, 33.3, 33.4, 49.1, 54.2, 56.1, 67.6, 68, 88; 379/59, 60, 62; 340/988, 989, 991; 342/46, 118, 357, 450, 458, 463; 364/443, 449, 460, 561